NON-SIMPLE ABELIAN VARIETIES IN A FAMILY: GEOMETRIC AND ANALYTIC APPROACHES

JORDAN S. ELLENBERG, CHRISTIAN ELSHOLTZ, CHRIS HALL, AND EMMANUEL KOWALSKI

Abstract. Let A_t be a family of abelian varieties over a number field k parametrized by a rational coordinate t, and suppose the generic fiber of A_t is geometrically simple. For example, we may take A_t to be the Jacobian of the hyperelliptic curve $y^2 = f(x)(x-t)$ for some polynomial f. We give two upper bounds for the number of $t \in k$ of height at most B such that the fiber A_t is geometrically non-simple. One bound comes from arithmetic geometry, and shows that there are only *finitely* many such t; but one has very little control over how this finite number varies as f changes. Another bound, from analytic number theory, shows that the number of geometrically non-simple fibers grows quite slowly with B; this bound, by contrast with the arithmetic one, is effective, and is uniform in the coefficients of f. We hope that the paper, besides proving the particular theorems we address, will serve as a good example of the strengths and weaknesses of the two complementary approaches.

Introduction

Given an algebraic family $\{A_t\}_{t\in\mathbb{Q}}$ of abelian varieties parametrized by a rational number t whose generic fiber has a certain property, it is natural to ask what one can say about the set of $t \in \mathbb{Q}$ such that A_t has the same property. One expects that in many cases this set will be "large" in some sense, even if the property in question is not a straightforward "algebraic" condition.

We consider in this context the property of geometric simplicity, which can be approached from several directions. In fact, in some sense, the main goal of this paper is to use this example to illustrate and compare different approaches, via arithmetic geometry and via analytic number theory. It turns out that neither is clearly preferable to the other, each method showing characteristic strengths and weaknesses, which we will try to emphasize. In this spirit, and for the sake of clarity, we do not always pursue the strongest possible conclusions.

More precisely, we will discuss the following two theorems, each of which is a special case of a more general theorem proved in the main body of the paper. Both concern the family of Jacobians A_t of hyperelliptic curves defined by affine equations

$$y^2 = f(x)(x-t)$$

for some squarefree polynomial $f \in \mathbb{Z}[X]$ of degree $2g$, $g \geqslant 1$. For $t \in \mathbb{Q}$ written $t = a/b$ with coprime integers a and b, let $H(t) = \max(|a|, |b|)$ be the height of t. Let then $S(B)$ denote the set of $t \in \mathbb{Q}$ with $H(t) \leqslant B$ such that A_t is *not* geometrically simple.

Theorem (Arithmetic geometry)**.** *There exists a constant $C(f)$, depending on f, such that*

$$|S(B)| \leqslant C(f) \tag{1}$$

2000 *Mathematics Subject Classification.* Primary 11G10; Secondary 11N35, 14K15, 14D05.

for all $B \geqslant 1$. In other words, there are only finitely many t for which A_t is not geometrically simple.

This is a special case of Theorem 9 in Section 1 and is elaborated on in Example 14 in Section 2.

Theorem (Analytic number theory)**.** *There exist absolute constants $C \geqslant 0$ and $D \geqslant 1$ such that we have*

$$|S(B)| \leqslant C(g^2 D(\log B))^{11g^2} \tag{2}$$

for all $B \geqslant 1$.

This is a special case of Theorem 24 in Section 3, where we have simplified the bound by worsening it somewhat. (For readers interested in this analytic approach but who are not familiar with abelian varieties, we have summarized enough information to understand the basic problem in an Appendix, which they may want to read now before starting Section 3).

The first theorem may initially appear much stronger. But note that in (1), we have no idea about the actual value of $C(f)$, in particular about how it may vary with f, whereas in the second theorem, the bound (2) is *effective* in terms of f. In particular this means we can deduce bounds for similar problems involving families with more than one parameter, e.g., for Jacobians of

$$y^2 = f(x)(x-t)(x-v),$$

for fixed square-free f of degree $2g-1$ and parameters t, $v \in k$. One can also deduce from (2) some upper bound for the smallest height of a t such that A_t is geometrically simple, namely there exists some t of height $\leqslant B$ for which A_t is geometrically simple, where

$$B = C'(D'g^4)^{11g^2}$$

for some constants $C' > 0$, $D' \geqslant 1$ (computable in terms of C and D).

The situation may be compared with the problem of counting rational points on a plane curve X of genus $\geqslant 2$. The theorem of Faltings shows that this set of points is finite, but it gives no effective bound for the heights of the solutions, and only estimates depending badly on X for the number of points. On the other hand, the method of Heath-Brown in [24] yields a completely explicit bound, depending only on the degree of X, for the number of points on X of height at most B.

Going further with the analogy, we may notice that Caporaso, Harris, and Mazur [4] have shown that if a certain conjecture of Lang [30] holds, then there is a bound *depending only on g* for the number of rational points on a curve of genus g over $\mathbb{Q}$. This suggests the following rather speculative question about the topic of the current paper:

Question 1. Is there an absolute constant C such that, for any squarefree polynomial $f \in \mathbb{Z}[x]$, there are at most C rational numbers t such that the Jacobian of $y^2 = f(x)(x-t)$ is geometrically non-simple?

If the question is relaxed to allow C to depend on the degree of f (i.e., the genus of the hyperelliptic curves under consideration), then Lang's conjecture implies an affirmative answer: as we shall see, the proof of Theorem 9 is based on showing that $S(B)$ maps injectively to the set of rational points on one of a finite set of curves of sufficiently large genus, where the number and genera of these curves are bounded in terms of $\deg(f)$.

One can be even more ambitious and ask the following purely geometric question:

Question 2. Is there an absolute constant C such that, for any squarefree polynomial $f \in \mathbb{C}[x]$ of degree at least 6, there are at most C complex numbers t such that the Jacobian of $y^2 = f(x)(x-t)$ is not simple?

Geometrically, we are asking whether there is an absolute bound on the number of complex intersection points between certain rational curves in $\mathcal{M}_g$ and the sublocus of $\mathcal{M}_g$ parametrizing curves whose Jacobians are non-simple. The difficulty arises from the fact that the non-simple locus is a countable union of proper subvarieties, so it is certainly not obvious a priori that there are finitely many $t \in \mathbb{C}$ for which A_t is non-simple. Indeed, when $g = 2$, the non-simple locus is a countable union of divisors, so a typical curve intersects this locus infinitely many times; this is the reason we require $\deg(f) \geqslant 6$.

Acknowledgments. We wish to thank F. Voloch for many helpful conversations. The first-named author's work was partially supported by NSF-CAREER Grant DMS-0448750 and a Sloan Research Fellowship.

Notation. As usual, $|X|$ denotes the cardinality of a set, and $\mathbb{F}_q$ is a field with q elements. For a number field k, $\mathbb{Z}_k$ denotes its ring of integers, and for a prime ideal $\mathfrak{p} \subset \mathbb{Z}_k$, $\mathbb{F}_\mathfrak{p}$ is the residue field $\mathbb{Z}_k/\mathfrak{p}$.

By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant" refers to any value of C for which this holds. It may depend on the set X, which is usually specified explicitly, or clearly determined by the context.

1. Methods from arithmetic geometry, I

In this section and the next we consider a field k which is finitely generated over the prime field, e.g., k could be a number field or a function field over a finite field.[1] We also assume that the characteristic of k, if positive, is not equal to 2.

The first conditions arise because we need to know that the following mild weakening of Mordell's conjecture holds for k:

Theorem 3. *With k as above, there is a constant $g_1(k)$ such that for any smooth projective curve C/k of genus $g > g_1(k)$, the set $C(k)$ of k-rational points on C is finite.*

Proof. At a minimum we must have $g \geqslant 2$, and if $\mathrm{char}(k) = 0$, then we may take $g_1(k) = 2$. If C is not defined over an algebraic closure of the prime field of k, then this is a combination of results of Manin–Grauert [33], [17] (for $\mathrm{char}(k) = 0$) and Samuel [36] (for $\mathrm{char}(k) > 0$). If $\mathrm{char}(k) = 0$ and C is defined over the algebraic closure of $\mathbb{Q}$, then the argument in the corollary of Theorem 1 of [34] reduces this to the celebrated theorem of Faltings [10]. The case which can force us to take $g_1(k) > 2$ is when $k = \mathbb{F}_q(X)$ for a smooth projective variety $X/\mathbb{F}_q$ and C is defined over $\mathbb{F}_q$. If $\mathbb{F}_q$ is algebraically closed in k, then elements of the complement $C(k) - C(\mathbb{F}_q)$ correspond to dominant maps $X \to C$ and repeated composition with the Frobenius $C \to C$ gives rise to an infinite subset of $C(k)$. However, the following

[1] These will be the only fields arising in the analytic section, and the reader can think of these as the most important.

proposition shows if we take $g_1(k) = \dim H^0(X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \Omega^1)$, there are no such elements, hence $C(k) = C(\mathbb{F}_q)$ is finite. □

Proposition 4. *Let $Y/\overline{\mathbb{F}}_q$ be a smooth projective curve of genus g. For any dominant map $f : X \to Y$ where $X/\overline{\mathbb{F}}_q$ is a smooth projective variety, we have $g \leqslant \dim H^0(X, \Omega^1)$.*

The following proof was suggested by J.F. Voloch.

Proof. If $f : X \to Y$ is inseparable, then there is a purely inseparable map of curves $Z \to Y$ through which f factors and such that $X \to Z$ is separable. Moreover, the genus of Y is at most the genus of Z, so up to replacing Y with Z we may assume f is separable. Then the pullback map of differentials

$$f^* : H^0(Y, \Omega^1) \to H^0(X, \Omega^1)$$

is an embedding (cf. [39, Theorem 1 in III.6.2]), and since $\dim(H^0(Y, \Omega^1)) = g$, the conclusion follows. □

Let now C/k be a smooth curve, and let $A/k(C)$ be a principally-polarized abelian variety of dimension g over the function field of C. Let ℓ be a prime which is invertible in k and let $A[\ell]$ be the ℓ-torsion of A.

There is an embedding of the group $G = \mathrm{Gal}(k(C)(A[\ell])/k(C))$ into $\Gamma = \mathrm{Aut}(A[\ell])$, where Aut is understood to refer to the group of linear automorphisms preserving the symplectic Weil pairing, up to a scalar. The subgroup of symplectic automorphisms of $A[\ell]$ is denoted Γ_0. We therefore have isomorphisms

$$\Gamma \simeq GSp(2g, \mathbb{F}_\ell), \qquad \Gamma_0 \simeq Sp(2g, \mathbb{F}_\ell)$$

(where $GSp(2g)$ is the group of symplectic similitudes, also sometimes written $CSp(2g)$ or even $SSp(2g)$.)

By the *geometric monodromy* of A *modulo* ℓ, we mean the image of the absolute Galois group of $k^s(C)$ in Γ_0. We say A has *big monodromy mod* ℓ if the geometric monodromy of A is the whole symplectic group Γ_0, so that $\Gamma_0 \leqslant G$. If v is a place of $k(C)$, we write A_v for the fiber over v of the Neron model of A over C and $G_v \leqslant G$ for the decomposition group. We say A_v has *big monodromy modulo* ℓ if A_v is an abelian g-fold and if $\Gamma_0 \leqslant G_v \leqslant G$. In all this, if ℓ is clear from the context, we may simply speak of *geometric monodromy*, or say that A or A_v *has big monodromy*, without specifying ℓ.

These notions are relevant for our basic problem because of the following sufficient criterion for geometric simplicity, which will be our main tool in this and the next section. This makes precise the fairly intuitive fact that a factorization of an abelian variety forces the monodromy group to preserve the factors, and hence is incompatible with having big monodromy; but because the factorization may exist only over an extension of k, and is valid only up to isogeny, this requires some care.

Proposition 5. *For any $g \geqslant 1$, there is a constant $\ell_1(g) \geqslant 1$ satisfying the following: if $\ell > \ell_1(g)$ and A/k is an abelian variety of dimension g over a field k such that A has big monodromy modulo ℓ, then A satisfies $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$ and in particular is geometrically simple.*

Proof. By a theorem of Chow, we have $\mathrm{End}_{\bar{k}}(A) = \mathrm{End}_{k^s}(A)$ for any abelian variety A/k (see [7, Th 3.19]), so it suffices to prove the corresponding statement with the endomorphism ring over k^s instead of over $\bar{k}$.

Next, for any A/k, note that the rank of the endomorphism ring $\mathrm{End}_{k^s}(A')$, as a $\mathbb{Z}$-module, is constant as A' runs over the isogeny class of A. If A is not geometrically simple, there is an abelian variety A' in this isogeny class which splits over $\bar{k}$ as $A_1 \times A_2$, with A_1, A_2 of dimension $\geqslant 1$. By the previous paragraph, this means in particular that $\mathrm{End}_{k^s}(A')$ contains a non-trivial endomorphism π satisfying $\pi^2 = \pi$ (e.g., the projection onto the non-trivial factor A_1), and then $\mathbb{Z}[\pi]$ is a rank-two $\mathbb{Z}$-submodule of $\mathrm{End}_{k^s}(A')$ and thus $\mathrm{End}_{k^s}(A) \neq \mathbb{Z}$ (since it has rank $\geqslant 2$). In particular, by contraposition, A is geometrically simple if $\mathrm{End}_{k^s}(A) = \mathbb{Z}$.

Now, let ℓ be a prime number such that some abelian variety A/k has big monodromy modulo ℓ and satisfies $\mathrm{End}_{k^s}(A) \neq \mathbb{Z}$. Then, by the theory of abelian groups, there is an endomorphism ψ in $\mathrm{End}_{k^s}(A)$ such that $\mathbb{Z}[\psi]$ is a rank-two $\mathbb{Z}$-submodule of $\mathrm{End}_{k^s}(A)$ and moreover $\mathrm{End}_{k^s}(A)/\mathbb{Z}[\psi]$ has no ℓ-torsion. The latter assumption implies that the image of $\mathbb{Z}[\psi]$ in $\mathrm{End}(A[\ell]) \simeq M_{2g}(\mathbb{F}_\ell)$ is a rank-two $\mathbb{F}_\ell$-submodule, because otherwise $\psi - m$ would be divisible by ℓ for some $m \in \mathbb{Z}$. More precisely, we may find ψ such that the image of ψ in $\mathrm{End}(A[\ell])$ does not lie in the scalar subgroup $\mathbb{F}_\ell^\times$.

Let K be the Galois closure of the splitting field of ψ (i.e., K is the fixed field of the subgroup of $\mathrm{Gal}(\bar{k}/k)$ fixing ψ) and let H be its Galois group of $K(A[\ell])/K$. There is a natural inclusion $H \to G$, where G is the monodromy group of A modulo ℓ.

Since the action of ψ on $A[\ell]$ commutes with H and ψ does not lie in the scalar subgroup $\mathbb{F}_\ell^\times \leqslant \mathrm{End}(A[\ell])$, Schur's Lemma implies that the subgroup $H \leqslant M_{2g}(\mathbb{F}_\ell)$ does not act absolutely irreducibly on $A[\ell]$. Since $G \cap \Gamma_0 = \Gamma_0$ does have this property (because of the big monodromy assumption), $H \cap \Gamma_0$ is a proper subgroup of Γ_0. Now, if $\ell > 3$, we know that Γ_0 is generated by its elements of order ℓ, because they generate a normal subgroup and $Z(\Gamma_0) = \{\pm 1\}$ is the only proper normal subgroup (see [43, Theorem 5]). Thus, there exists at least one element σ of order ℓ in the complement $G - H$. In particular, the σ-orbit of H in the permutation representation on G/H has ℓ elements, hence we find that $[G : H] \geqslant \ell$.

On the other hand, the Galois group $\mathrm{Gal}(K/k)$ acts faithfully on the free $\mathbb{Z}$-module $\mathrm{End}_K(A)$, so that it is isomorphic to a finite subgroup F of $\mathrm{GL}(n, \mathbb{Z})$ for some $n \leqslant 2g$. By a theorem of Minkowski, F injects into $\mathrm{GL}(n, \mathbb{Z}/3\mathbb{Z})$ (see for instance [40]) and thus its order is bounded by a constant depending only on g. Let $\ell_1(g)$ be this constant. Since Galois theory gives

$$[G : H] \leqslant |\mathrm{Gal}(K/k)|,$$

it follows from this and the previous paragraph that

$$\ell \leqslant [G : H] \leqslant |F| \leqslant \ell_1(g),$$

as desired. □

Our first (and most general) approach to the problem mentioned in the introduction uses some deep group-theoretic results of Liebeck–Saxl [32] and Guralnick [19], in order to apply Proposition 5. This is contained in the following result:

Proposition 6. *If $g_1 \geqslant 0$ is a constant, then there is a constant $\ell_2(g_1)$ satisfying the following. If $\ell > \ell_2(g_1)$ and $X \to C$ is a geometric Galois cover with group $G = \mathrm{Sp}(2g, \mathbb{F}_\ell)$, then for any proper subgroup $H < G$, the genus of X/H is at least g_1.*

Proof. In the case where f is tamely ramified (for instance in characteristic zero), this follows from [32, Corollary 2 to Theorem 1], and in the general case, this follows from [19, Theorem 1.5]. □

Remark 7. The constant $\ell_2(g_1)$ is conjectured to be independent of g_1 ([19, Conjecture 1.6]), and in the tame case this follows from [13, Theorem A].

What is required for Proposition 6 is a very thorough understanding of the maximal proper subgroups of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$. As written, the results in [32] and [19] both use the classification of finite simple groups. More precisely, the proof of Corollary 9.5 in [19] uses Theorem 1 of [32] which in turn rests on the classification-dependent Theorem 4.1 of [31]. However, we learned from Guralnick [20] that Magaard has an unpublished proof of Theorem 1 of [32] which does not use the classification.

Proposition 6 forms the main content of the following proposition.

Proposition 8. *If $\ell > \ell_2(g_1(k))$ and A has big monodromy mod ℓ, then A_v has big monodromy mod ℓ for all but finitely many $v \in C(k)$.*

Proof. Let X/k be the smooth curve with function field $k(C)(A[\ell])$. The map of curves $X \to C$ is generically Galois with group G containing Γ_0. Let v be a point in $C(k)$ and let w be a point in X lying over v with decomposition group $G_v \leqslant \Gamma$. If $H \leqslant G$ is a subgroup not containing Γ_0, and $G_v \leqslant H$, then the image of w in the quotient curve X/H has degree $[G_v : G_v \cap H] = 1$ over v, hence is a k-rational point of X/H. In particular, to prove the theorem it suffices to show that X/H has genus greater than $g_1(k)$ for any proper subgroup $H < G$ because then Theorem 3 implies that

$$\bigcup_{H<G} (X/H)(k)$$

is finite. But this is exactly Proposition 6 applied to the proper subgroup $H \cap \Gamma_0$ of Γ_0. □

We can now deduce the following concrete application:

Theorem 9. *Let k be an infinite field of finite type over the prime field, for instance a number field. Let $g \geqslant 1$ be an integer, and let $f \in k[X]$ be a squarefree polynomial of degree $2g$.*

Let A be the Jacobian of the hyperelliptic curve of genus g over $k(t)$ with affine model

$$y^2 = f(x)(x - t).$$

Then there are only finitely many $t \in k$ such that A_t is not geometrically simple.

Proof. By a result of J-K. Yu and the third author [21], A has big monodromy modulo ℓ for any $\ell \geqslant 3$. Choosing $\ell > \max(2, \ell_1(g), \ell_2(g_1(k)))$ yields the desired result by combining Proposition 5 and Proposition 8. □

In the theorems above we have used the fact that A has big monodromy modulo some prime ℓ in order to show that almost all the fibers A_v have big monodromy modulo the same ℓ. It is worth pointing out that the hypothesis that A_v has big monodromy modulo a sufficiently large fixed ℓ_0 actually implies that it has big monodromy modulo almost all ℓ, although we will only prove it for global fields.

Proposition 10. *Suppose k is a global field, i.e. a number field or a function field of a curve over a finite field. If A_v has big monodromy modulo ℓ_0, for some $\ell_0 \geqslant 5$, then there is a constant $\ell_3(A_v)$ so A_v has big monodromy modulo ℓ for every prime $\ell > \ell_3(A_v)$.*

Proof. If A_v has big monodromy for $\ell_0 \geqslant 5$, then the ℓ_0-adic monodromy group of A_v contains $\mathrm{Aut}(T_{\ell_0}A) \simeq \mathrm{Sp}(2g, \mathbb{Z}_{\ell_0})$ (see [38, Lemme 1]). Therefore, if k is a number field, then [37, 2.2.7] and [38, Théorème 3] imply that for every sufficiently large ℓ, the ℓ-adic monodromy group of B contains $\mathrm{Sp}(2g, \mathbb{Z}_\ell)$. If k is a function field over a finite field, then one can apply [38, 8.2] to deduce a similar statement. □

It is worth noting here that this method does *not* allow the bound $\ell_3(A_v)$ to be chosen independently of A_v. To prove such a uniform bound over a rational function field, for example, would require showing that the Siegel modular varieties parametrizing abelian g-folds with 'H-level structure' contain no unexpected rational curves; this can be carried out when $g = 1$, since the Siegel modular variety is just a curve (see [6]) but seems difficult in general. A theorem of Nadel [35] proves such a result (as a special case of a much more general theorem) when H is the trivial subgroup of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$.

2. Methods from arithmetic geometry, II

In the special case of families of hyperelliptic curves contemplated in the present paper, we can also obtain results using easier group theory in place of Proposition 6, as we now explain. Again, we will use Proposition 5 to obtain geometric simplicity.

We continue with the notation introduced in the previous section except that now we must work in characteristic zero, so we assume k is a finitely generated over a number field. This implies that Theorem 3 is valid with $g_1(k) = 2$.

First of all, we remark that when A has big monodromy modulo a sufficiently large ℓ and at least three fibers where the reduction is not potentially good, then one can show that A_v has big monodromy modulo ℓ via the results in [22], which require only Thompson's classification of so-called quadratic pairs [44].

By restricting A further, we can make our work even simpler, while still proving a general enough result to obtain the theorems stated in the introduction. For this, we say A *degenerates simply* at v if the identity component of A_v is the extension of an abelian variety by a one-dimensional torus and if the component group of A_v has order prime to ℓ. There are only finitely many v where A degenerates simply. From the group-theoretic point of view, this geometric condition is useful because of the following fact:

Lemma 11. *With notation as above, if A degenerates simply at v, then the inertia group $I_v \leqslant G_v$ is generated by a transvection.*

Proof. By [18, (2.5.4) and Corollaire 3.5.2], I_v is generated by a unipotent element τ satisfying $\dim((\tau - 1)A[\ell]) \leqslant 1$, so τ is either a transvection or is trivial. Moreover, $A[\ell]$ does not split over the strict henselization of the local field $k(C)_v$ because the component group of A_v has order prime to ℓ (cf. [18, (11.1.3)]), hence $k(C)(A[\ell])$ ramifies over v and $\tau \neq 1$ is a transvection, as claimed. □

We will also use here the following group-theoretic lemma, the potential significance of which is clear from the previous one.

Lemma 12. *If $\ell \geqslant 3$, then a subgroup of $Sp(2g, \mathbb{F}_\ell)$ which contains ℓ^{2g-1} transvections is the whole of $Sp(2g, \mathbb{F}_\ell)$.*

Proof. This follows immediately from a theorem of Brown and Humphries [3], which gives a criterion for a set of transvections to generate the symplectic group $Sp(2g, \mathbb{F}_\ell)$. More precisely, recall that there is a natural bijection between cyclic groups generated by transvections and lines in $\mathbb{F}_\ell^{2g}$; namely, we take the group generated by τ to the 1-dimensional space $(\tau - 1)(\mathbb{F}_\ell^{2g})$. Let $S \subset \mathbb{P}(\mathbb{F}_\ell^{2g})$ be a set of subgroups generated by transvections. Let $G(S)$ be the graph with set of vertices S and with edges given by those pairs $(s_1, s_2) \in S \times S$ such that the space spanned by s_1 and s_2 (thought of as lines in $\mathbb{F}_\ell^{2g}$) is not isotropic. Then [3] shows that (for $\ell \geqslant 3$), S generates G if and only if the elements of S span $\mathbb{F}_\ell^{2g}$, and if $G(S)$ is connected. If the lines in S fail to span all of $\mathbb{F}_\ell^{2g}$, then obviously

$$|S| \leqslant \frac{\ell^{2g-1} - 1}{\ell - 1}.$$

On the other hand, if $G(S)$ is the disjoint union of two subgraphs G_1 and G_2, the subspaces of $\mathbb{F}_\ell^{2g}$ spanned by the vertices of G_1 and G_2 must be mutually orthogonal, so in particular the union of these vector spaces contains at most $(\ell^{2g-1} - 1)/(\ell - 1)$ lines. In either case, the number of transvections contained in S is at most $\ell^{2g-1} - 1$. □

Now we deduce the following:

Proposition 13. *Let k be a field finitely generated over a number field, let C/k be a smooth projective curve, and let $A/k(C)$ be a principally-polarized abelian g-fold. Suppose $\ell \geqslant 3$ is a prime such that A has big monodromy modulo ℓ and that A degenerates simply at*

$$\left\lceil \frac{2(\ell^{2g} - 1)}{(\ell^g - \ell^{g-1})^2} \right\rceil$$

or more places. Then A_v has big monodromy modulo ℓ for all but finitely many $v \in C(k)$.

Proof. We can assume that the places where A degenerates simply are in $C(k)$, because the conclusion will even be stronger after extending scalars to a field of definition of those places. Then, let again X/k be the smooth curve with function field $k(C)(A[\ell])$. The map of curves $X \to C$ is generically Galois with group G contained in Γ. Again, we use Theorem 3, applied to the curves X/H as H ranges over proper subgroups of Γ_0. As in the proof of Proposition 8, and because $g_1(k) = 2$ now, it suffices to show that all such X/H have genus at least 2.

Fix a proper subgroup $H < \Gamma_0$ and let Y/k be the quotient curve X/H. Suppse v is a point where A degenerates simply and let $\tau \in I_v$ be a generator. There is an action of τ on the sheets of $Y \times_k k^s$ which is exactly the permutation action on the cosets of Γ_0/H: the orbits correspond to the points of $Y \times_k k^s$ over v and the size of an orbit is the ramification index. Every orbit has 1 or ℓ elements and the coset gH is fixed by τ if and only if $g^{-1}\tau g$ lies in H. In particular, the computation of the ramification of $Y \to C$ at v is reduced to a problem about the conjugates of transvections in G.

By Lemma 12, we have

$$\frac{|\tau^G \cap H|}{|\tau^G|} \leqslant \frac{\ell^{2g-1} - 1}{\ell^{2g} - 1},$$

so there are at least

$$\frac{\ell^{2g-2}(\ell - 1)}{\ell^{2g} - 1}[G : H]$$

points of $Y \times_k k^s$ over v of ramification degree ℓ. Therefore, if we write m for the number of v in $C(k)$ where A degenerates simply, then from the Riemann-Hurwitz formula we have that

$$2g(Y) - 2 \geqslant [G : H]\Big(\frac{m\ell^{2g-2}(\ell-1)^2}{\ell^{2g}-1} + 2g(C) - 2\Big).$$

In particular, the right hand side is positive since $m(\ell^g - \ell^{g-1})^2 > 2(\ell^{2g} - 1)$, hence $Y = X/H$ has genus at least two. □

Example 14. When A is the Jacobian of

$$y^2 = f(x)(x - t)$$

with $\deg(f) = 2g$, we observe that, for $\ell \geqslant 3$, A degenerates simply at every prime v in $k(t)$ corresponding to the specialization of t to a root of $f(x)$. A priori, one could apply the description of the monodromy of A about v given in [22, Section 5] to deduce that it is a transvection, which is why we want it to be simply degenerate (see Lemma 11), but one can also perform a geometric computation to check this directly.

The fact that A_v is the extension of an abelian variety by a one-dimensional torus, for instance, from [1, §9.2, Example 8]. The key point is that the fiber of the curve over v is smooth away from a single ordinary double point.

To compute the order of the component group of A_v, one must compute the minimal regular model of the curve over v, which a straightforward calculation reveals to be the union of curve C_1 of genus $g-1$ and a curve C_2 of genus 0 (Remark IV.7.7 and Example IV.7.7.1 of [42] give a nice concrete treatment of the blowing-up process required for this computation). Moreover, C_1 and C_2 intersect in two points, from which it follows that one has the divisor intersection numbers $C_1^2 = C_2^2 = -2$ and $C_1 \cdot C_2 = 2$ (cf. [42, Proposition IV.8.1]). Using this information one applies [1, §9.6, Theorem 1] to deduce that the component group of A_v is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

So when $g \geqslant 2$, we immediately recover Theorem 9 using Proposition 13. (The case $g = 1$ is standard; see for instance [6].)

3. Methods from analytic number theory

The analytic approach to our problem is based on the conjunction of two sieves: the sieve for Frobenius of the last-named author (see [27]), which is a version of the large sieve, and a generalisation of Gallagher's larger sieve [14]. The prototype of this approach was described in [27, Prop. 6.3], which used a standard large sieve instead of the larger sieve. The latter is much more efficient here.

This combination of two sieves is quite appealing, and it may be of interest in other applications. Although we do not know of any previous use of the large sieve to set up a larger sieve, the second-named author has, in earlier work, used the larger sieve to prepare for application of the large sieve (see [9]).

The sieve arises because, instead of the "big monodromy" argument in Proposition 5, we will detect non-simple abelian varieties by means of the following alternate criterion:

Proposition 15. *Let k be a number field and A/k be an abelian variety. Let $\mathfrak{p} \subset \mathbb{Z}_k$ be a prime ideal of k with residue field $\mathbb{F}_\mathfrak{p}$ such that A has good reduction at $\mathfrak{p}$. If the abelian variety $A_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$ obtained by reduction of A modulo $\mathfrak{p}$ is geometrically simple, then so is A.*

Proof. This is a tautology, given the theory of reductions of abelian varieties: if A is not geometrically simple, there exists an isogeny

$$A \simeq A_1 \times A_2$$

with $\dim A_1, \dim A_2 \geqslant 1$, which is defined over some finite Galois extension k'/k. The factors A_1 and A_2 have good reduction at $\mathfrak{p}$, and so, after reducing, we obtain a corresponding non-trivial factorization for $A_{\mathfrak{p}}$ defined over the residue extension of k'/k at $\mathfrak{p}$. □

Remark 16. It is well-known that there exist integral polynomials which are irreducible over $\mathbb{Q}$ but which are reducible modulo every prime (this is due to Hilbert; see, e.g., [2], where it is shown that such polynomials exist of every non-prime degree). Similarly, there are examples of geometrically simple abelian varieties defined over a number field which are not geometrically simple modulo any prime (see the review [12] by R. Fisher of a paper by C. Adimoolam, and the results of Hashimoto and Murabayashi [16]). It would be interesting to know if the analogue of the finiteness statement (1) holds for the set $S'(B)$ of parameters of height $\leqslant B$ for which A_t is not simple modulo all primes.

Sieve methods, in particular the large sieve, will be used to detect factorizations of abelian varieties over finite fields (much as they can be used to detect irreducible polynomials), and thus we will proceed by applying Proposition 15 at many different primes.

We first give a new formulation of Gallagher's sieve in number fields (the works of Hinz [25] and Goldberg [15] have other versions, as does a work in progress of D. Zywina). The terminology "larger sieve" arises because this statement is most efficient when trying to control the size of a set which does not intersect a very large number of residue classes modulo a set of primes.

Proposition 17. *Let $k/\mathbb{Q}$ be a number field, let $B > 0$ be a constant, and let $\mathcal{A}$ be a finite set of elements of k such that $H(a) \leqslant B$ for all $a \in \mathcal{A}$, where H denotes the height in k, normalized as described below.*

Let S be a finite set of prime ideals in the ring of integers $\mathbb{Z}_k$. If the order of the image of $\mathcal{A}$ under the reduction map $k \to \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is $\leqslant \nu(\mathfrak{p})$ for all $\mathfrak{p} \in S$, then we have

$$|\mathcal{A}| \leqslant \frac{\displaystyle\sum_{\mathfrak{p}\in S} \log N\mathfrak{p} - \log(2^{[k:\mathbb{Q}]}B^2)}{\displaystyle\sum_{\mathfrak{p}\in S} \frac{\log N\mathfrak{p}}{\nu(\mathfrak{p})} - \log B - \log(2^{[k:\mathbb{Q}]}B^2)},$$

provided *the denominator in either of these two expressions is positive.*

Remark 18. For many applications, the weaker estimate

$$|\mathcal{A}| \leqslant \frac{\displaystyle\sum_{\mathfrak{p}\in S} \log N\mathfrak{p}}{\displaystyle\sum_{\mathfrak{p}\in S} \frac{\log N\mathfrak{p}}{\nu(\mathfrak{p})} - 2\log(2^{[k:\mathbb{Q}]}B^2)}, \tag{3}$$

also valid when the denominator is positive, is sufficient. Indeed, this is what we will use.

We indicate which definition of the height we consider, since there are competing normalizations; we follow [41, VIII.5], i.e., our H is the same as Silverman's H_k. Thus let M_k be

the set of places of k, defined as in [41, VIII.5, p. 206] (the set of absolute values on $k^\times$, which coincide with the standard absolute values on $\mathbb{Q}$ when restricted to $\mathbb{Q}^\times$), and let $|\cdot|_v$ denote the absolute value associated with $v \in M_k$.

For $a \in k$, the height of a is defined by

$$H(a) = \prod_{v \in M_k} \max(1, |a|_v^{n_v})$$

where n_v is the local degree at v, i.e., $n_v = [k_v : \mathbb{Q}_v]$, where k_v and $\mathbb{Q}_v$ are the completions of k (resp. $\mathbb{Q}$) with respect to the metric defined by $\|\cdot\|_v$ (in particular $n_v = 2$ if v is a complex place).

We will need the following easy and well-known results:

$$H(a) = H(a^{-1}) \qquad H(ab) \leqslant H(a)H(b) \qquad H(a+b) \leqslant 2^{[k:\mathbb{Q}]} H(a)H(b) \tag{4}$$

for all a, $b \in k^\times$. We also recall that if $v \in M_k$ is a non-archimedean place, associated with a prime ideal $\mathfrak{p}$, then we have

$$|a|_v^{n_v} = (N\mathfrak{p})^{-v_\mathfrak{p}(a)}, \tag{5}$$

where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation and $N\mathfrak{p} = |\mathbb{F}_\mathfrak{p}| = |\mathbb{Z}_k/\mathfrak{p}\mathbb{Z}_k|$ is the order of the residue field.

We also comment briefly on the reduction map $k \to \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$: if $a \in k$ and $v_\mathfrak{p}(a) < 0$ (i.e., if $\mathfrak{p}$ "divides the denominator" of a), then the image of a modulo $\mathfrak{p}$ is the point at infinity (denoted ∞) in $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$. We write simply $a \equiv \infty \pmod{\mathfrak{p}}$ to indicate that this is the case.

Proof of Proposition 17. The proof is very similar to the original argument of Gallagher [14]. Let

$$\Delta = \prod_{\substack{a,b \in \mathcal{A} \\ a \neq b}} H(a-b)$$

which is real number $\geqslant 1$. We will compare upper and lower bounds for Δ to obtain the larger sieve inequality. By (4), we first have the easy upper bound

$$\Delta \leqslant (2^{[k:\mathbb{Q}]} B^2)^{|\mathcal{A}|(|\mathcal{A}|-1)}. \tag{6}$$

On the other hand, we bound the height from below as follows: by (4) again, switching to the inverse to use (5) with positive valuations, we have

$$\Delta = \prod_{a \neq b} H((a-b)^{-1}) \geqslant \prod_{a \neq b} \prod_{\mathfrak{p} \in S_{a,b}} (N\mathfrak{p})^{v_\mathfrak{p}(a-b)}$$

where

$$S_{a,b} = \{\mathfrak{p} \in S \mid v_\mathfrak{p}(a) \geqslant 0, \quad v_\mathfrak{p}(b) \geqslant 0\}.$$

It follows that

$$\begin{aligned}
\log \Delta &\geqslant \sum_{a \neq b} \sum_{\substack{\mathfrak{p} \in S_{a,b} \\ a \equiv b \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}) \\
&= \sum_{a \neq b} \sum_{\substack{\mathfrak{p} \in S \\ a \equiv b \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}) - \sum_{a \neq b} \sum_{\substack{\mathfrak{p} \in S \\ a \equiv b \equiv \infty \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}) \\
&= L_1 - L_2, \qquad \text{(say)},
\end{aligned}$$

(since if $\mathfrak{p} \in S - S_{a,b}$, then $a \equiv b \pmod{\mathfrak{p}}$ implies that both a and b reduce to ∞).

Now, for all $\mathfrak{p} \in S$ and $\alpha \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, define

$$R_\mathfrak{p}(\alpha) = |\{a \in \mathcal{A} \mid a \equiv \alpha \pmod{\mathfrak{p}}\}|.$$

We obtain

$$\begin{aligned} L_1 &= \sum_{\mathfrak{p} \in S} (\log N\mathfrak{p}) \sum_{\substack{a \neq b \\ a \equiv b \pmod{\mathfrak{p}}}} 1 \\ &= \sum_{\mathfrak{p} \in S} (\log N\mathfrak{p}) \sum_{\substack{a,b \in \mathcal{A} \\ a \equiv b \pmod{\mathfrak{p}}}} 1 - |\mathcal{A}| \sum_{\mathfrak{p} \in S} \log N\mathfrak{p} \\ &= \sum_{\mathfrak{p} \in S} (\log N\mathfrak{p}) \sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} R_\mathfrak{p}(\alpha)^2 - |\mathcal{A}| \sum_{\mathfrak{p} \in S} \log N\mathfrak{p}. \end{aligned}$$

However, by Cauchy-Schwarz, and by definition of $\nu(\mathfrak{p})$, we have the familiar lower bound

$$\sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} R_\mathfrak{p}(\alpha)^2 \geqslant \frac{\Big(\sum_{\alpha \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} R_\mathfrak{p}(\alpha)\Big)^2}{\nu(\mathfrak{p})} = \frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})},$$

and therefore we obtain

$$L_1 \geqslant \sum_{\mathfrak{p} \in S} \Big\{ \frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})} - |\mathcal{A}| \Big\} \log N\mathfrak{p}.$$

Now we bound L_2 from above in order to conclude; we have for all a and b in $\mathcal{A}$ the rather trivial estimate

$$\sum_{\substack{\mathfrak{p} \in S \\ a \equiv b \equiv \infty \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}) \leqslant \sum_{\substack{\mathfrak{p} \in S \\ a \equiv \infty \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}) \leqslant \log H(a) \leqslant \log B,$$

and finally by putting things together, we obtain

$$\sum_{\mathfrak{p} \in S} \Big\{ \frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})} - |\mathcal{A}| \Big\} \log N\mathfrak{p} - |\mathcal{A}|^2 (\log B) \leqslant \log H(\Delta) \leqslant |\mathcal{A}|(|\mathcal{A}| - 1) \log(2^{[k:\mathbb{Q}]} B^2).$$

Simplifying by $|\mathcal{A}|$ and re-arranging gives the result. □

When applying this proposition, we assume some upper bound on $\nu(\mathfrak{p})$, on average over S, and estimate the right-hand side of (3). In our case, $\nu(\mathfrak{p})$ will be quite small (less than $(N\mathfrak{p})^{1-\delta}$ for some $\delta > 0$), so that if the set S is chosen to be

$$S = \{\mathfrak{p} \subset \mathbb{Z}_k \mid N\mathfrak{p} \leqslant x\}$$

for some parameter $x \geqslant 2$ (as is typically the case), the first sum in the denominator grows fairly rapidly as x grows.

The strength of the final estimates stems from this, but in a way which is rather surprising compared with the large sieve (for instance): it will come from the fact that one can choose x quite small to make the denominator positive; then the numerator is also fairly small, hence so is $\mathcal{A}$, but the actual size of the denominator is, in fact, of little significance (in other words, it is not really a "saving factor").

From this sketch, one can guess that the only really delicate issue that may arise is if one tries to have estimates uniform in terms of k, for then one is led directly to the difficult issue of showing that there are sufficiently many prime ideals with small norm.

In order to clarify the mechanism, we define

$$\beta_k(x;\delta) = \min\Big\{t \geqslant 2 \mid \sum_{N\mathfrak{p}\leqslant t} (N\mathfrak{p})^{-1+\delta} \geqslant x\Big\}, \qquad \text{for } t \geqslant 2, \quad 0 \leqslant \delta < 1, \tag{7}$$

which, intuitively, quantifies the "convergence to equilibrium" in the Prime Ideal Theorem for k. Note in particular that

$$\beta_k(x;\delta) \geqslant \min\{n \geqslant 2 \mid \text{ there is some prime ideal of norm } n\},$$

since *any* sum over primes of smaller norm is zero by definition.

If k is considered to be fixed, we can deduce, by summation by parts, from the Prime Ideal Theorem that

$$\sum_{N\mathfrak{p}\leqslant t} (N\mathfrak{p})^{-1+\delta} = \frac{t^\delta}{\log t^\delta} + O\Big(\log\frac{1}{\delta} + \frac{t^\delta}{(\log t^\delta)^2}\Big),$$

for $\delta > 0$ and $t \geqslant 2$ with $t^\delta \geqslant 2$, where the implied constant depends on k only. It then follows easily that

$$\beta_k(x;\delta) \ll (2x\log x)^{1/\delta} \tag{8}$$

for $x \geqslant 2$, where the implied constant depends only on k.

Corollary 19. *Let $k/\mathbb{Q}$ be a number field and let $\mathcal{A}$ be a finite set of elements of k such that $H(a) \leqslant B$ for all $a \in \mathcal{A}$, and such that, for all prime ideals $\mathfrak{p}$ in $\mathbb{Z}_k$, the order of the image of $\mathcal{A}$ under the reduction map $k \to \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is $\leqslant \nu(\mathfrak{p})$ where*

$$\nu(\mathfrak{p}) \leqslant C(N\mathfrak{p})^{1-\gamma^{-1}}(\log N\mathfrak{p})$$

for some constants $C > 0$ and $\gamma \geqslant 1$.

Then we have

$$|\mathcal{A}| \leqslant 2C[k:\mathbb{Q}]\beta_k\Big(3C\log(2^{[k:\mathbb{Q}]}B^2);\gamma^{-1}\Big)(\log 2^{[k:\mathbb{Q}]}B^2)^{-1}.$$

Proof. Write $\delta = \gamma^{-1}$. Applying Proposition 17 (in the form of (3)) with S taken to be the set

$$S = \{\mathfrak{p} \mid N\mathfrak{p} \leqslant x\}$$

for some $x \geqslant 2$ to be determined later, the denominator of (3) is

$$-2\log(2^{[k:\mathbb{Q}]}B^2) + \sum_{\mathfrak{p}\in S}\frac{\log N\mathfrak{p}}{\nu(\mathfrak{p})} \geqslant -2\log(2^{[k:\mathbb{Q}]}B^2) + C^{-1}\sum_{N\mathfrak{p}\leqslant x}(N\mathfrak{p})^{-1+\delta}.$$

Thus if we take

$$x = \beta_k\Big(3C\log(2^{[k:\mathbb{Q}]}B^2);\delta\Big),$$

then the definition (7) shows that the denominator is $\geqslant \log(2^{[k:\mathbb{Q}]}B^2)$.

We bound the numerator, on the other hand, rather wastefully in terms of k:

$$\sum_{N\mathfrak{p}\leqslant x}\log N\mathfrak{p} \leqslant [k:\mathbb{Q}](\log x)\pi(x) \leqslant 2[k:\mathbb{Q}]x,$$

(by the Brun-Titchmarsh or Chebychev upper-bound for $\pi(x)$). The result is then a direct translation of Proposition 17. □

Under various assumptions, one can easily transform this into concrete results. For simplicity, we do this for a fixed number field; there, using (8), we obtain:

Corollary 20. *Let k be a fixed number field. With assumption as in Corollary 19, we have*

$$|\mathcal{A}| \ll (\log 2^{[k:\mathbb{Q}]}B^2)^{\gamma-1}(6C\log(9C\log 2^{[k:\mathbb{Q}]}B))^{\gamma},$$

for all $B \geqslant 2$, the implied constant depending only on k.

Example 21. For $k = \mathbb{Q}$, using a lower-bound such as

$$\pi(x) \geqslant \frac{1}{6}\frac{x}{\log x}$$

for $x \geqslant 2$ (which follows, e.g., from [23, p. 342]), one gets easily (and rather wastefully) that

$$\beta_{\mathbb{Q}}(x;\delta) \leqslant \Big(\frac{12x}{\delta}\log\frac{2x}{\delta}\Big)^{1/\delta},$$

and hence

$$|\mathcal{A}| \leqslant 2\Big(\frac{36C}{\delta}\Big)^{1/\delta}(\log 2B^2)^{1/\delta-1}\Big(\log\frac{6C}{\delta}\log 2B^2\Big)^{1/\delta},$$

under the assumption of Corollary 19 for $k = \mathbb{Q}$.

Now we come to the application to the splitting of Jacobians in our hyperelliptic families. We use the following result, which is itself proved using a version of the large sieve, to derive assumptions such as those in Corollary 19, involving the type of conditions in Proposition 15.

Proposition 22. *Let $\mathbb{F}_q$ be a finite field with q elements, let $g \geqslant 1$ be an integer and let $f \in \mathbb{F}_q[X]$ be a squarefree polynomial of degree $2g$. For $t \in \mathbb{F}_q$, let A_t be the Jacobian of the hyperelliptic curve C_t with affine equation*

$$C_t \,:\, y^2 = f(x)(x-t).$$

Then we have

$$|\{t \in \mathbb{F}_q \mid f(t) \neq 0 \text{ and } A_t \text{ is not geometrically simple}\}| \ll g^2 q^{1-\gamma^{-1}}(\log q) \tag{9}$$

where $\gamma = 4g^2 + 2g + 4$ and the implied constant is absolute.

Proof. Fix a prime number $\ell \neq p$. For $t \in \mathbb{F}_q$, we let P_t denote the numerator of the zeta function of C_t, which is the integral polynomial of degree $2g$ given by

$$P_t = \det(1 - TF \mid H^1(A_t, \mathbb{Z}_\ell)),$$

where $H^1(A_t,\mathbb{Z}_\ell) \simeq H^1(C_t,\mathbb{Z}_\ell)$ is the first étale cohomology group of A_t or C_t (this is the "spectral interpretation" of the zeros of the zeta function of C_t).

Let G_t be the Galois group of the splitting field of P_t. We write W for the group which is the "generic" value of G_t, namely the Weyl group of the symplectic group $Sp(2g)$, or more concretely, the group of order $2^g g!$ consisting of signed permutation matrices in $GL(n,\mathbb{Z})$.

From the application of the sieve for Frobenius in [28, Remark after Th. 8.13], it follows that

$$|\{t \in \mathbb{F}_q \mid f(t) \neq 0 \text{ and } G_t \not\simeq W\}| \ll g^2 q^{1-\gamma^{-1}}(\log q),$$

where $\gamma = 4g^2 + 2g + 4$ and the implied constant is *absolute* (the earlier result in [27, Th. 6.2] has $\gamma = 4g^2 + 3g + 5$ instead, which is virtually indistinguishable; it also misses the g^2 factor, due to a slip in the final step of the estimate).

Precisely, this result trivially implies (9) if "geometrically simple" is replaced by "simple", since an isogeny (over $\mathbb{F}_q$) of the type

$$A_t \simeq A_1 \times A_2 \tag{10}$$

with $\dim A_1$, $\dim A_2 \geqslant 1$, implies that

$$P_t = \det(1 - TF \mid H^1(A_1, \mathbb{Z}_\ell)) \det(1 - TF \mid H^1(A_2, \mathbb{Z}_\ell)), \tag{11}$$

where both factors are integral polynomials of degree $\geqslant 1$, which can certainly not occur if P_t has Galois group W.

To claim the result stated in the geometric context, one must exclude factorizations as above which hold only over a finite extension of $\mathbb{F}_q$. For fixed g, one can adapt straightforwardly the corresponding qualitative argument of Chavdarov [5, Th. 2.1, Lemma 5.3]. The dependency on g might be worse than what we claim when applying this directly, but for $g \geqslant 5$ (at least), one can use instead the following elementary argument exploiting the size of the Galois group. First, one can show (see [29, Prop. 2.4, (2)]) that $G_t \simeq W$ and $g \geqslant 5$ imply that the only multiplicative relations between zeros of P_t must follow from the Riemann Hypothesis, i.e., if $(\alpha_1, \dots, \alpha_{2g})$ are the inverse roots of P_t, we have $\mathbb{Q} \otimes_{\mathbb{Z}} R = T$, where

$$R = \{(n_i) \in \mathbb{Z}^{2g} \mid \prod_i \alpha_i^{n_i} = 1\},$$

$$T = \{(m_i) \in \mathbb{Q}^{2g} \mid \sum_j m_j = 0, \text{ and } m_i = m_j \text{ if } \alpha_i = \bar{\alpha}_j\}.$$

Now if (10) holds over $\mathbb{F}_{q^m}$, $m \geqslant 1$, it is easy to see that there must be a relation $\alpha_j^m = \alpha_k^m$ with $j \neq k$, and this corresponds to a relation $(n_i) \in R$ with $n_i = 0$ except $n_j = n_k = m$, which is incompatible with the definition of T. □

Remark 23. The uniformity in g is a nice additional feature of the sieve method, but it is not necessarily crucial here; the uniformity in terms of the characteristic of $\mathbb{F}_q$ is what matters for the later use of this proposition.

It is worth noting one common feature of the geometric and analytic approaches here: the proof of Proposition 22 depends crucially on the same result of J-K. Yu (reproved in [21]) concerning the monodromy modulo ℓ of our hyperelliptic families, over finite fields.

Theorem 24. *Let $k/\mathbb{Q}$ be a number field, $g \geqslant 1$ an integer and $f \in k[X]$ a squarefree polynomial of degree $2g$. For $t \in k$, not a zero of f, let A_t be the Jacobian of the hyperelliptic curve with affine equation*

$$y^2 = f(x)(x - t).$$

For $B \geqslant 1$, let

$$S(B) = \{t \in k \mid H(t) \leqslant B \text{ and } A_t \text{ is not geometrically simple}\}.$$

Then there exists an absolute constant $D \geqslant 0$ such that, for $B \geqslant 2$, we have

$$|S(B)| \ll (\log 2^{[k:\mathbb{Q}]} B^2)^{\gamma - 1} (g^2 D \log\log 2^{[k:\mathbb{Q}]} B)^\gamma,$$

with $\gamma = 4g^2 + 2g + 4$, where the implied constant depends only on k.

Proof. The basic observation is that, if $t \in S(B)$ then for any prime ideal $\mathfrak{p}$, $t \pmod p \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is either a zero of f modulo $\mathfrak{p}$, or ∞, or else ($f(t)$ being non-zero modulo $\mathfrak{p}$ so that A_t has good reduction modulo $\mathfrak{p}$, and its fiber over $\mathfrak{p}$ then being not geometrically simple), $t \pmod \mathfrak{p}$ lies in the set $\Omega_\mathfrak{p}$ defined by (9) for f relative to $q = N\mathfrak{p}$.

Hence the image of $S(B)$ modulo $\mathfrak{p}$ has cardinality $\nu(\mathfrak{p})$ with

$$\nu(\mathfrak{p}) \leqslant 2g + 1 + |\Omega_\mathfrak{p}| \ll g^2 (N\mathfrak{p})^{1-\gamma^{-1}} (\log N\mathfrak{p}),$$

where the implied constant is absolute by Proposition 22. Thus Corollary 20 directly implies the result. □

Remark 25. In an extremely narrow range, the large sieve (as used originally in [27]) is better than the larger sieve. Indeed, as discussed with many examples in [8], the original larger sieve is better when the number of permitted residue classes (i.e., the size of $\Omega_\mathfrak{p}$, in our case) is smaller than half of $N\mathfrak{p}$ (this is not quite true anymore in our inequality because of the term $\log 2^{[k:\mathbb{Q}]} B^2$ in the denominator). Proposition 22 clearly shows that we can not prove this[2] unless $N\mathfrak{p}$ is (roughly) larger than $\delta^{-1/\delta}$ (with $\delta \asymp g^2$). But the bound in Proposition 22 also becomes trivial for g not much beyond this point, so the range of applicability where the large sieve would be the best is very small.

Appendix: survey of abelian varieties for analytic number theorists

While the basic information about abelian varieties that we use will certainly be well-known to readers more familiar with the methods of Sections 1 and 2, this is less likely to be the case for readers whose interests lie more in the direction of analytic number theory and sieves. In order to motivate the basic problem for these readers, we summarize here briefly some background information, which we hope will suffice to make accessible the contents of Section 3 for such readers.

The simplest case of abelian varieties is that of elliptic curves; although our basic question of geometric simplicity is not of interest in this setting (any elliptic curve is geometrically simple), a basic knowledge of elliptic curves can help motivate and understand the general theory. We refer for this to Silverman's book [41], and to the summary in [26, §11.10], which may also be helpful.

Let k be a number field (for instance, $k = \mathbb{Q}$). An abelian variety A defined over k is, first of all, a *proper variety* over k; that is, we may think of A as a subset of projective space over k cut out by some set of homogeneous equations in the coordinates. (In practice, though, one almost never writes down these equations!) What makes A an abelian variety is the presence of a *group law*: a map from $A \times A$ to A which is given by polynomials in the coordinates, and satisfies the usual group axioms – associativity, presence of an inverse, and so on. (One might compare A with the more familiar example of SL_n /k, which is also determined as a subset of k^{n^2} by a set of equations, and which also has a group operation which is polynomial in the matrix entries. The difference is that A is cut out by equations in projective space, while SL_n is cut out by equations in the affine space k^{n^2}.)

Since k is contained in $\mathbb{C}$, we can ask not only about the group of solutions over k to the defining equations of A, but about the set of complex solutions, denoted $A(\mathbb{C})$. Write g for

[2] It may be true, for all we know.

the dimension of A. It is known that A is necessarily isomorphic to $\mathbb{C}^g/\Lambda$ for some lattice $\Lambda \simeq \mathbb{Z}^{2g} \subset \mathbb{C}^g$; in the 1-dimensional case $g = 1$, A is an elliptic curve over k.

In particular, it follows that the subgroup $A[n]$ of elements of order dividing n in A, for any integer $n \geqslant 1$, is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, and moreover the fact that A is defined over k easily implies that the coordinates of elements in $A[n]$ are algebraic numbers, which all together generate a finite Galois extension $k(A[n])$ of k.

Algebraic curves provide a natural source of abelian varieties via the construction of the *Jacobian*, which over $\mathbb{C}$ goes back to Jacobi, and over k to Weil. To each non-singular algebraic curve C/k of genus g, one can attach a natural abelian variety $J(C)$ over k of dimension g. One nice feature of Jacobians is that they are *principally polarized*: this is a kind of self-duality which imposes on $J(C)[n]$ a natural perfect pairing

$$J(C)[n] \times J(C)[n] \to \boldsymbol{\mu}_n \simeq \mathbb{Z}/n\mathbb{Z}$$

where $\boldsymbol{\mu}_n$ denotes the group of n-th roots of unity.

In fact, the action of $\mathrm{Gal}(\bar{k}/k)$ on the coordinates of $k(A[n])$ is not merely linear, but compatible with the symplectic pairing above; thus it provides a representation

$$\mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(A[n]) \simeq GSp(2g, \mathbb{Z}/n\mathbb{Z}).$$

The primary examples of abelian varieties treated in this paper are Jacobians of curves; in any event, all the abelian varieties we consider are for simplicity assumed to be principally polarized.

The most delicate issue for Section 3 is that of reductions of an abelian variety modulo prime ideals of $\mathbb{Z}_k$. Suffice it to say here that this can be defined for all but finitely many prime ideals of k (the "primes of bad reduction"), and that if concrete equations for A are given so that, modulo $\mathfrak{p}$, the resulting equations still define a smooth algebraic variety, then the reduction coincides pretty much with the naïve notion of looking at solutions of the equations with coefficients in extensions of the residue field $\mathbb{Z}_k/\mathfrak{p}$.

Now our basic problem takes root in the following definition: an abelian variety A/k is *simple* if and only if there is no nontrivial abelian variety B over k which is a subvariety of A, except A itself. It is *geometrically simple* if it remains simple even when considered as an abelian variety over $\mathbb{C}$.

Implicit in the notion of geometric simplicity is that, for most lattices $\Lambda \in \mathbb{C}^g$, the quotient $\mathbb{C}^g/\Lambda$ is not an abelian variety. It is merely a complex torus; the condition that it embeds as an algebraic subvariety of projective space imposes very strong restrictions on Λ (originally described by Riemann.) In particular, if $\mathbb{C}^g/\Lambda$ is an abelian variety, it is not usually possible to find a subspace $V \in \mathbb{C}^g$ such that $\Lambda \cap V$ is a lattice in V and $V/(\Lambda \cap V)$ is an abelian variety. In other words, abelian varieties over $\mathbb{C}$ are "typically" simple.

Now the question considered in this paper is essentially the following: we form a family, parameterized by elements in k, of curves; then we have an associated family of Jacobian varieties, and we ask: *how frequent is it that those abelian varieties are not geometrically simple*?

The basic approach in Section 3 is founded on the following fact: if an abelian variety A/k is not geometrically simple, then its reduction modulo a prime ideal $\mathfrak{p}$ has the same property (which is intuitive enough). Moreover, a result going back in principle to Poincaré shows that a non-trivial subvariety $B \subset A$ is "essentially" a direct factor, i.e., we have

$$A \simeq B \times C$$

for some other abelian subvariety C, up to finite groups ("up to isogeny"). This is the property (10) which leads to the factorization (11) which we use to control the occurence of non-geometrically simple varieties.

References

[1] Bosch, S., Lütkebohmert, W. and Raynaud, M. Néron models. Ergebnisse der Math. (3), 21, Springer-Verlag, 1990.

[2] Brandl, R. Integer polynomials that are reducible modulo all primes. American Math. Monthly 93 (1986), 286–288.

[3] Brown, R. and Humphries, S. Orbits under symplectic transvections, I. *Proc. London Math. Soc.* (3) 52 (1986), no. 3, 517–531.

[4] Caporaso, L., Harris, J. and Mazur, B. Uniformity of rational points. *J. Amer. Math. Soc.* 10 (1997), no. 1, 1–35.

[5] Chavdarov, N. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Math. J.* 87 (1997), 151–180.

[6] Cojocaru, A.C. and Hall, C.J. Uniform results for Serre's theorem for elliptic curves. *Int. Math. Res. Not.* 2005, no. 50, 3065–3080.

[7] Conrad, B. Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. *Enseign. Math.* (2) 52 (2006), no. 1-2, 37–108.

[8] Croot, E.S. and Elsholtz, C. Variants of Gallagher's larger sieve. *Acta Math. Hung.* 103 (2004), 243–254.

[9] Elsholtz, C. The inverse Goldbach problem. *Mathematika* 48, 151–158 (2003).

[10] Faltings, G. Endlichkeitssätze für abelsche Variatäten über Zahlkörpern. *Invent. math.* 73 (1983), 349–366.

[11] Faltings, G. and Wüstholz, G. Rational points. Aspects of Mathematics, Vieweg 1986.

[12] Fisher, R.J. Review of "A note on good reduction of simple abelian varieties", by C. Adimoolam. Math Reviews, MR 0447259.

[13] Frohardt, D. and Magaard, K. Composition factors of monodromy groups. *Ann. of Math. (2)* 154 (2001) no. 2, 327–345.

[14] Gallagher, P.X. A larger sieve. Acta Arith. 18 (1971), 77–81.

[15] Goldberg, E.L. Electrostatic sieve. *Mathematika* 23 (1976), no. 1, 51–56.

[16] Hashimoto, K. and Murabayashi, N. Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two. *Tohoku Math. J.* (2) 47 (1995), no. 2, 271–296.

[17] Grauert, H. Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper. *Inst. Hautes Études Sci. Publ. Math.* No. 25 (1965), 131–149.

[18] Grothendieck, A. "Modèles de Néron et monodromie" in *Groupes de monodromie en géométrie algébrique, I*, Seminaire de Géometrié Algébrique du Bois-Marie 1967–1969, (SGA 7 I), no. 9, Lecture Notes in Math. **288**, Springer, Berlin, 1972, 313–523.

[19] Guralnick, R. Monodromy groups of coverings of curves. *Galois groups and fundamental groups,* 1–46, Math. Sci. Res. Inst. Publ., 41, Cambridge Univ. Press, Cambridge, 2003.

[20] Guralnick, R. (Personal communication). 2007.

[21] Hall, C. Big symplectic or orthogonal monodromy modulo ℓ. *Duke Math J.*, vol. 141 (2008), no.1, 179–203

[22] Hall, C. Maximal subgroups of classical groups containing a quadratic element (In progress).

[23] Hardy, G.H. and Wright, E.M. An introduction to the theory of numbers. 5th Edition, Oxford Univ. Press, 1979.

[24] Heath-Brown, D.R. The density of rational points on curves and surfaces. *Ann. of Math.* (2), 155(2) (2002) 553–595.

[25] Hinz, J. Square-Free values of cubic polynomials in algebraic number fields. *J. of Number Theory* 32 (1986), 203–320.

[26] Iwaniec, H. and Kowalski, E. Analytic number theory. Colloquium Publ. 53, A.M.S, 2004.

[27] Kowalski, E. The large sieve, monodromy and zeta functions of curves. *J. reine angew. Math.*, 601 (2006), 29–69.

[28] Kowalski, E. The large sieve and its applications: arithmetic geometry, random walks and discrete groups. Cambridge Tracts in Math. 175, Cambridge University Press 2008 (to appear).
[29] Kowalski, E. The large sieve, monodromy and zeta functions of algebraic curves, II: Independence of the zeros. Preprint(2008).
[30] Lang, S. Hyperbolic and Diophantine analysis. *Bull. Amer. Math. Soc. (N.S.)* 14 (1986), no. 2, 159–205.
[31] Liebeck, M. On the orders of maximal subgroups of the finite classical groups. *Proc. London Math. Soc.* (3) 50 (1985), no. 3, 426–446.
[32] Liebeck, M. and Saxl, J. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc.* (3) 63 (1991), no. 2, 266–314.
[33] Manin, Ju. I. Rational points on algebraic curves over function fields. *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963), 1395–1440.
[34] Martin-Deschamps, M. La construction de Kodaira-Parshin. *Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84).* Astérisque No. 127 (1985), 261–273.
[35] Nadel, A. The nonexistence of certain level structures on abelian varieties over complex function fields *Ann. of Math. (2)* 129 (1989), no. 1, 161–178.
[36] Samuel, P. Compléments à un article de Hans Grauert sur la conjecture de Mordell. *Inst. Hautes Études Sci. Publ. Math.* No. 29 (1966), 55–62.
[37] Serre, J.-P. Résumé des course de 1984–1985 Œuvres. Collected papers. IV. (French) 1985–1998. Springer-Verlag, Berlin, 2000.
[38] Serre, J.-P. Letter to Marie-France Vignéras Œuvres. Collected papers. IV. (French) 1985–1998. Springer-Verlag, Berlin, 2000.
[39] Shafarevich, I. R. *Basic algebraic geometry. 1. Varieties in projective space.* Second edition. Translated from the 1988 Russian edition and with notes by Miles Reid. Springer-Verlag, Berlin, 1994.
[40] Silverberg, A. and Zarhin, Y. Semistable reduction and torsion subgroups of abelian varieties. *Annales de l'Institut Fourier*, v. 45 (1995), no. 2, 403–420.
[41] Silverman, J. *The arithmetic of elliptic curves.* Graduate Text in Math. 106, Springer 1986.
[42] Silverman, J. *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.
[43] Steinberg, R. Lectures on Chevalley groups. Notes prepared by John Faulkner and Robert Wilson. Yale University, New Haven, Conn., 1968.
[44] Thompson, J. Quadratic pairs. *Actes du Congrés International des Mathématiciens (Nice, 1970)*, Tome 1, pp. 375–376.

Department of Mathematics, University of Wisconsin, 480 Lincoln Drive, Madison, WI 53705 USA
E-mail address: ellenber@math.wisc.edu

Department of Mathematics, Royal Holloway, University of London, Egham, TW20 0EX Surrey, UK
E-mail address: christian.elsholtz@rhul.ac.uk

Department of Mathematics, University of Michigan at Ann Arbor, Michigan, USA
E-mail address: hallcj@umich.edu

ETH Zürich – D-MATH, Rämistrasse 101, 8092 Zürich, Switzerland
E-mail address: kowalski@math.ethz.ch